Detecting and Counteracting Benign Faults and Malicious Attacks in Cyber Physical Systems

Israel Koren
University of Massachusetts at Amherst
Amherst, MA 01003, USA
koren@ecs.umass.edu

Abstract— **The use of cyber-physical system (CPS) is rapidly expanding and many of their applications require a highly reliable and secure implementation as they control critical infrastructures or even life-critical devices. Unfortunately, current techniques for achieving high reliability and security incur high overheads. In particular, integrating countermeasures against security attacks is problematic as security threats are often not well defined, evolve continuously, and as a result, many CPSs often remain vulnerable. We propose to exploits the physical plant state information to enhance both reliability and security. Our approach, which monitors the controlled plant state trajectory, allows for tunable fault-tolerance as well as detection of malicious attacks, and it achieves these at a low overhead. The plant state space consists of safe and marginal state subspaces. In the safe subspace the CPS will continue its safe operation even if the worst case control signal is applied. In contrast, any erroneous control applied when the plant state is marginal, may lead to a catastrophic system failure. Such an erroneous control output may be due to either a benign fault or a malicious security attack. As most of the time the plant will be deep within its safe subspace, we can avoid using expensive redundancy techniques and thus, reduce the computational load while still guaranteeing safe operation. When a marginal state of the plant is detected, it will signal the potential presence of a "natural" fault or malicious attack. Our scheme will counter this by switching to a critical mode involving higher levels of redundancy to combat natural failures as well as alternative mechanisms to defeat malicious attacks.**

A major challenge in our approach is to determine, in real-time, whether the current state of the physical plant is deep within its safe sub-space or is marginal. We have used various machine learning techniques for classifying the state and our results indicate that with a reasonable number of entries in a lookup table and with a short execution time, the required classification can be performed efficiently.

CURRICULUM VITAE

Israel Koren is a Professor of Electrical and Computer Engineering at the University of Massachusetts, Amherst and a fellow of the IEEE. He has been a consultant to companies like IBM, Analog Devices, Intel, AMD and National Semiconductors. His research interests include Fault-Tolerant systems, secure cryptographic devices, Computer architecture and computer arithmetic. He publishes extensively and has over 300 publications in refereed journals and conferences. He is the author of the textbook "Computer Arithmetic Algorithms," 2nd Edition, A.K. Peters, Ltd., 2002, and a co-author of the textbook "Fault Tolerant Systems," Morgan-Kaufman, 2007.

Web site: http://www.ecs.umass.edu/ece/koren/

REFERENCES

[1] Y. Xu, I. Koren and C.M. Krishna, ``AdaFT: A Framework for Adaptive Fault Tolerance for Cyber-Physical Systems," ACM Transactions on Embedded Computing Systems (TECS),} pp. 79.1-79.25, April 2017.

978-1-5386-5683-9/18/$31.00 ©2018 IEEE